

GOVERNANCE DOCS

IEC 62443-2-1:2024

Gap Assessment Report

IEC 62443-2-1:2024 IACS Security Programme for Asset Owners

Delta Water Controls (sample)

The SCADA and PLC environment for three treatment plants, and the remote access that supports it.

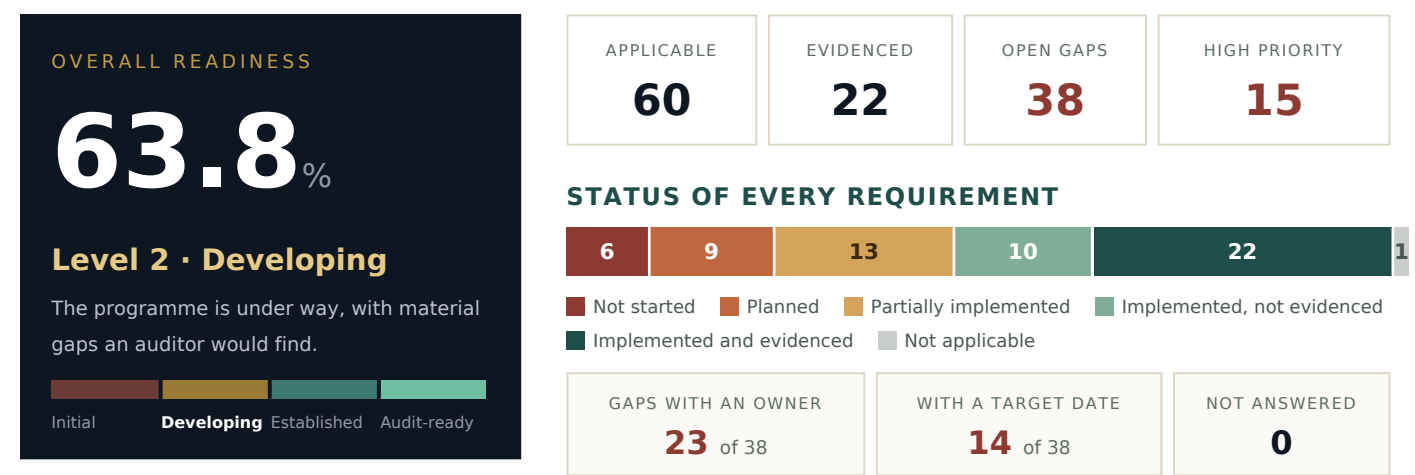
ASSESSED	25 September 2026
EDITION	2-1:2024 (second edition), with 62443-3-2:2020 zoning and 62443-3-3:2013 security levels
IN SCOPE	61 requirements, 60 applicable
PROFILE	Manufacturing and industrial · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Delta Water Controls (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Delta Water Controls (sample) stands against IEC 62443



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 63.8% against IEC 62443 across 60 applicable controls. 22 of them are implemented and evidenced.
- Most open gaps: Scope, roles and conformity, with 6 at 43%. Strongest area: Security levels at 100%.
- 10 controls are operating but not evidenced. Collecting their records alone lifts the score to 67.9% (+4.1 points), the cheapest gain available.
- 15 gaps are high priority (not started or only planned); 5 of them are in SPE 6 - User access control.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 5 high-priority gaps in SPE 6 - User access control	Operations Manager	Session Management and Login Control Standard
2	MEDIUM	Adopt and tailor the Network Architecture and Data Flow Diagram Set, which closes 2 open gaps	To assign	Network Architecture and Data Flow Diagram Set
3	LOW	Evidence the 10 controls that already operate (+4.1 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

At 63.8% readiness, the organization should immediately establish user access controls to mitigate critical operational security vulnerabilities.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization's self-assessment against IEC 62443 places cybersecurity readiness at level 2 of 4, with an overall score of 63.8% and 38 open gaps. The primary operational exposure lies in user access control and event detection, where fundamental safeguards have not started. To protect industrial operations, senior leadership requires board support to allocate dedicated operational resources over the next 90 days. This focus will allow you to establish baseline access controls, formalize incident logging, and assign owners to all outstanding gaps.

WHERE YOU STAND

Your self-assessment against IEC 62443 shows an overall score of 63.8%, placing the organization at readiness level 2 of 4, named Developing. Out of 60 applicable requirements, 38 open gaps remain, including 15 high priority gaps. While 22 requirements are implemented and evidenced, 10 are implemented without evidence, 13 are partially implemented, 9 are planned, and 6 are not started. Furthermore, 23 gaps have an assigned owner and 14 have target completion dates, showing active but incomplete program governance.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment indicates strong technical baselines in areas such as Security levels at 100% and System integrity and availability at 87.5%. In contrast, core operational practices are lagging. User access control scored lowest at 20.8% with 6 open gaps, followed by Event and incident management at 40% with 5 open gaps. This pattern means the industrial control environment lacks documented safeguards around authentication, user privileges, and event monitoring. Without these controls, the organization faces significant exposure to untracked access and undetected incidents in daily operations.

WHERE TO FOCUS FIRST

You should first address the unstarted high priority items within User access control and Event and incident management. Specifically, implement documented procedures for Session and login controls, Joiners, movers and leavers, and Detection and monitoring. Additionally, documenting evidence for the 10 requirements that are already implemented will raise the overall score from 63.8% to 67.9%. Finishing partially implemented controls will then advance the score to 78.8%, providing a structured path to close critical operational vulnerabilities.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Implement Core User Access and Lifecycle Controls USER 1.c Session and login controls · USER 2.b Joiners, movers and leavers · USER 2.c Access review	Uncontrolled sessions, unmanaged personnel changes, and unreviewed permissions leave systems open to unauthorized operational access. Establishing these controls stops inappropriate access from dormant accounts or untracked users.	Draft the IACS Joiners Movers and Leavers Procedure to regulate personnel access changes.	IACS Joiners Movers and Leavers Procedure IEC 62443 Toolkit – 117 IACS Cybersecurity Templates	30 DAYS
2 Collect Evidence for Implemented Component and Configuration Measures SC.5 Compensating measures for legacy assets · CM 1.3 Configuration settings · COMP 1 Component hardening and portable media	Ten controls are already functioning in practice but lack documented verification. Formalizing evidence validates existing practices and immediately increases the overall score to 67.9%.	Collate records into the Configuration Baseline Register and Hardening Baseline Checklists.	Configuration Baseline Register IEC 62443 Toolkit – 117 IACS Cybersecurity Templates	30 DAYS
3 Establish Event Detection and Logging Standards EVENT 1.a Detection and monitoring · EVENT 1.b Logging	Without active event detection and logging, unauthorized activity across the industrial network remains invisible. Timely detection is essential to contain security incidents before they affect plant operations.	Adopt the IACS Logging Standard across critical industrial components.	IACS Logging Standard IEC 62443 Toolkit – 117 IACS Cybersecurity Templates	60 DAYS
4 Define System Boundaries and Coordinate with the ISMS SC.4 Relationship with the ISMS · SC.2 System under consideration defined	Unclear system boundaries and disconnected governance create blind spots across industrial assets. Aligning the industrial program with the broader management system clarifies accountability.	Publish the System under Consideration Boundary Statement to define asset scope.	System under Consideration Boundary Statement IEC 62443 Toolkit – 117 IACS Cybersecurity Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Draft and approve the IACS Joiners Movers and Leavers Procedure to regulate access changes.
- Establish session management rules using the Session Management and Login Control Standard.
- Gather evidence for operating controls to populate the Configuration Baseline Register.

DAYS 31 TO 60

- Deploy event monitoring requirements defined in the IACS Event Detection and Monitoring Standard.
- Implement baseline logging across industrial network devices using the IACS Logging Standard.
- Conduct an initial access review recorded in the Access Review and Recertification Record.

DAYS 61 TO 90

- Document industrial boundaries using the System under Consideration Boundary Statement.
- Establish governance alignment using the Security Programme and ISMS Coordination Procedure.
- Assign responsible owners and target dates to all remaining unassigned open gaps.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope, roles and conformity	2 1 2 1 1	43%	3 2 1
Risk assessment, zones and conduits	4 1 3	72%	0 4 1
Security levels	3	100%	0 0 0
SPE 1 - Organizational security measures	3 1 2 5	70%	3 1 2
SPE 2 - Configuration management	1 1 2	75%	1 0 1
SPE 3 - Network and communications security	2 1 1	69%	0 2 1
SPE 4 - Component security	2 1	83%	0 0 2
SPE 5 - Protection of data	1 1 3	75%	1 1 0
SPE 6 - User access control	3 2 1	21%	5 0 1
SPE 7 - Event and incident management	1 1 2 1	40%	2 2 1
SPE 8 - System integrity and availability	1 3 1	88%	0 1 0

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		63.8%
Evidence what already runs 10 requirements		67.9% +4.1
Finish what is partly in place 13 requirements		78.8% +10.9
Implement what is planned 9 requirements		90.0% +11.2
Start what has not begun 6 requirements		100.0% +10.0

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Network Architecture and Data Flow Diagram Set		2
IACS Security Programme Charter and Objectives		2
OT and IT Governance Interface Procedure		2
Legacy and Unsupported Asset Compensating Measures Procedure		2
Zone and Conduit Partitioning Procedure		2
IACS Wireless Security Standard		2

All of these are in the IEC 62443 Toolkit (117 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 6

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.4	Relationship with the ISMS	Scope, roles and conformity	Compliance Lead	Security Programme and ISMS Coordination Procedure · ISMS Delta Register
SC.6	Maturity assessed, not just presence	Scope, roles and conformity	HR Manager 7 Jan 2027	Maturity Level Assessment Procedure · Security Programme Maturity Assessment Workbook
USER 1.c	Session and login controls	SPE 6	Operations Manager	Session Management and Login Control Standard · Legacy and Unsupported Asset Compensating Measures Procedure
USER 2.b	Joiners, movers and leavers	SPE 6	To assign	IACS Joiners Movers and Leavers Procedure
USER 2.c	Access review	SPE 6	HR Manager 21 Jan 2027	Access Review and Recertification Record
EVENT 1.a	Detection and monitoring	SPE 7	Risk Manager 10 Dec 2026	IACS Event Detection and Monitoring Standard · IACS Logging Standard

HIGH Planned · 9

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
SC.2	System under consideration defined	Scope, roles and conformity	Operations Manager 24 Dec 2026	System under Consideration Boundary Statement · Network Architecture and Data Flow Diagram Set
ORG 1.2	Background checks	SPE 1	Compliance Lead 10 Dec 2026	Personnel Screening and Background Check Policy
ORG 1.3	Security roles and responsibilities	SPE 1	Operations Manager 4 Feb 2027	Security Roles Responsibilities and Authorities · OT and IT Governance Interface Procedure
ORG 2.3	Secure development and support	SPE 1	HR Manager 26 Nov 2026	Secure Development and Support Assurance Procedure · Integration and Commissioning Security Handover Checklist

CM 1.2	Infrastructure drawings and documentation	SPE 2	Operations Manager	Infrastructure Drawings and Documentation Control Procedure · Network Architecture and Data Flow Diagram Set
DATA 1.c	Safety system configuration mode	SPE 5	Operations Manager 12 Nov 2026	Safety System Configuration Mode Control Procedure
USER 1.a	Identification and authentication	SPE 6	Risk Manager 10 Dec 2026	IACS Identity and Access Management Policy · User Identity and Access Rights Register +1 more
USER 1.b	Software and service accounts	SPE 6	Operations Manager 21 Jan 2027	Software Service Account Standard · Password and Credential Management Standard
EVENT 1.b	Logging	SPE 7	Operations Manager 7 Jan 2027	IACS Logging Standard

MEDIUM Partially implemented · 13

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.3	Accountability retained	Scope, roles and conformity	To assign	IACS Security Programme Charter and Objectives · OT and IT Governance Interface Procedure
SC.7	Certification expectations set	Scope, roles and conformity	IT Manager 24 Dec 2026	Conformity Evidence Register · IACS Security Programme Charter and Objectives
ZCR.2	Zones and conduits established	Risk assessment, zones and conduits	Compliance Lead	Zone and Conduit Partitioning Procedure · Zone and Conduit Register +1 more
ZCR.3	Business and IACS assets separated	Risk assessment, zones and conduits	Compliance Lead	Network Segmentation Standard · IACS Demilitarised Zone Design Pattern Guide
ZCR.6	Detailed risk assessment	Risk assessment, zones and conduits	To assign	Detailed Cybersecurity Risk Assessment Procedure · Detailed Cybersecurity Risk Assessment Report +2 more
ZCR.7	Cybersecurity requirements specification	Risk assessment, zones and conduits	To assign	Cybersecurity Requirements Specification
ORG 1.5	Security responsibilities training	SPE 1	Operations Manager	Security Responsibilities Training Plan and Competence Matrix · Training Record Register
NET 2	Secure wireless access	SPE 3	Risk Manager 29 Oct 2026	IACS Wireless Security Standard · Wireless Asset and Address Register

NET 3	Secure remote access	SPE 3	Operations Manager	Secure Remote Access Policy and Procedure · Remote Access Authorisation Register
DATA 1.e	Cryptography and key management	SPE 5	Risk Manager	Cryptographic Controls and Key Management Standard
EVENT 1.c	Event analysis and reporting	SPE 7	HR Manager 26 Nov 2026	Event Analysis Procedure · Event Reporting Procedure and Interfaces
EVENT 1.d	Incident response	SPE 7	Operations Manager	IACS Incident Response Plan · Incident Classification and Severity Matrix +1 more
AVAIL 2.b	Restores tested	SPE 8	To assign	Restoration Test Plan and Record

LOW Implemented, not evidenced · 10

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SC.5	Compensating measures for legacy assets	Scope, roles and conformity	To assign	Legacy and Unsupported Asset Compensating Measures Procedure · Security Programme Element Applicability Statement
ZCR.5	Temporary, wireless and externally connected devices	Risk assessment, zones and conduits	To assign	Zone and Conduit Partitioning Procedure · IACS Wireless Security Standard +1 more
ORG 2.1	Security risk mitigation	SPE 1	To assign	Risk Treatment Plan · IACS Cybersecurity Risk Management Procedure
ORG 2.2	Discovery of security anomalies	SPE 1	To assign	Security Assessment and Anomaly Discovery Procedure · Event Analysis Procedure
CM 1.3	Configuration settings	SPE 2	To assign	Configuration Settings Standard · Configuration Baseline Register
NET 1.b	Network autonomy	SPE 3	To assign	Network Autonomy and Disconnection Procedure · Network Time Distribution Standard
COMP 1	Component hardening and portable media	SPE 4	To assign	IACS Component Hardening Standard · Hardening Baseline Checklists +1 more
COMP 3	Patch management	SPE 4	To assign	IACS Security Patch Management Procedure · Patch Status and Validation Register +1 more
USER 2.a	Authorization and least privilege	SPE 6	To assign	Authorization and Privilege Elevation Procedure
EVENT 1.e	Vulnerability handling	SPE 7	To assign	IACS Vulnerability Handling Procedure

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com